Before the
United States Department of State
Washington, D.C. 20520

In the matter of
the Report of the Working Group on Internet Governance

COMMENTS OF VERISIGN, INC.

Brian Cute **Vice President, Government Relations** **VeriSign, Inc.** **1666 K Street, N.W.** **Washington, D.C. 20006** **Tel. 202.973.6615** **E-mail: bcute@verisign.com**	**Shane Tews** **Senior Washington Representative** **VeriSign, Inc.** **1666 K Street, N.W.** **Washington, D.C. 20006** **Tel. 202.973.6603** **E-mail: stews@verisign.com**
Michael Aisenberg **Director, Government Relations** **VeriSign, Inc.** **1666 K Street, N.W.** **Washington, D.C. 20006** **Tel. 202.973.6611** **E-mail: maisenberg@verisign.com**	**Anthony Rutkowski** **Vice President, Regulatory Affairs** **VeriSign Communications Services Div.** **21355 Ridgetop Circle** **Dulles VA 20166-6503** **Tel: 1 703.948.4305** **mailto:trutkowski@verisign.com**

I. INTRODUCTION

Pursuant to Public Notice published in the Federal Register on June 27, 2005, VeriSign, Inc. ("VeriSign") submits these comments to the Department of State ("Department"), International Telecommunications Advisory Committee, in response to the Department's request for public comments on the report of the Working Group on Internet Governance ("WGIG"). VeriSign has a substantial interest in the progress and outcome of the WGIG and its parent United Nations' activity, the World Summit on the Information Society (WSIS).[1] This interest emanates from significant business activities in the infrastructure of the global information technology system and networks, and attendant participation as a leading industry voice in policy activities regarding the evolution of these networks.

For more than a decade, VeriSign has provided an array of large-scale, ultra-high availability, trusted intelligent infrastructures that enable signalling, security, identity management, directory, financial transaction, and fraud management capabilities for communications, commerce, and content. These capabilities span an exhaustive array of network based business and consumer services – including Internet, Web, traditional voice telephony, wireless, Voice over Internet Protocol (VoIP), multimedia, next generation networks, and sales transactions. VeriSign operates through multiple divisions with 45 offices around the world.

As part of these commercial infrastructure support services, VeriSign operates the largest independent telecommunications SS7 (Signalling System No. 7) Intelligent Network based infrastructure in the U.S. for a large number of wireline, wireless, cable, and VoIP providers. VeriSign also provides the most robust and highest performance IP-enabled signalling, directory, security, and transaction services infrastructures in the world.

As part of the global public IP-enabled services intelligent infrastructure, VeriSign provides several parts of the most operationally critical name resolution services together with the associated directory support systems. These critical parts include:

- Two of the 13 IETF RFC-based Domain Name System "root" zone servers that point to the top-level domain name servers. One of these servers includes the primary A-root server which was designated to distribute the master root zone file to all of the root zone servers. (VeriSign also operates the J-root server). Because these servers are so important to the routing of Internet Protocol packets and are continuously subject to attack, VeriSign maintains an operations center to monitor the availability of the globally distributed root servers and to coordinate outage responses with other root server operators.
- VeriSign provides highly robust "backend" infrastructure for securely operating and maintaining the two largest generic top level domains (gTLDs) – .com and .net. VeriSign's infrastructure resources supporting these domains consists of a

[1] World Summit on the Information Society, United Nations, www.itu.int/wsis.

constellation of 18 geographically-dispersed DNS servers located in North America, Europe, and Asia. In response to the identification of additional geographic regions of emerging growth in Internet usage, VeriSign announced plans in April 2005 to install additional resolution servers over the next two years in Africa, the Middle East, Central and Eastern Europe to enhance Internet stability, security, and resolution speed within these regions.

Despite the continued rapid growth in .com and .net registrations—41.1 million active .com and .net domain name registrations at the end of the first quarter of 2005, an 8 percent increase over fourth quarter 2004—VeriSign maintains 100 percent operational accuracy and stability of both domains and has done so for more than seven years running.

- VerriSign has also encouraged and maintained industry "mindshare" leadership in DNS technical communities in important new next generation platforms such as secure DNS (DNS SEC), maintenance systems (EPP), telephone number resolution (ENUM), distributed directories (IRIS), and Universal Resource Names (URNs). As part of this fiduciary role over many years, VeriSign expert technical staff have led many technical and industry standards groups, written open source specifications, contributed freely available running code, and implemented the next generation products on high availability platforms.

II. THE REPORT OF THEWORKING GROUP ON INTERNET GOVERNANCE

VeriSign strongly supports the WGIG report principle that "the stable and secure functioning of the Internet" is of paramount importance and that its work and "recommendations aiming to improve current governance arrangements" should be assessed against this principle.[2]

A. Working definition of Internet governance

The WGIG report puts forward the following working definition of Internet governance: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision–making procedures, and programmes that shape the evolution and use of the Internet."[3] The WGIG report goes on to specify that "Internet governance includes more than Internet names and addresses, issues dealt with by the Internet Corporation for Assigned Names and Numbers (ICANN): it also includes other significant public policy issues, such as critical Internet resources, the security and safety of the Internet, and developmental aspects and issues pertaining to the use of the Internet."[4]

---

[2] Report of the Working Group on Internet Governance, pp. 3-4; also see WSIS Declaration of Principles, paras. 48-50 (WSIS-03/GENEVA/DOC/4-E).
[3] Report of the Working Group on Internet Governance, p. 4.
[4] Id.

The working definition of Internet governance is sufficiently broad, by design, to accommodate the interest of the various actors who should play active, collaborative roles in addressing issues of Internet governance on a forward going basis. It must be kept in mind, however, that the proposed definition of Internet governance, and indeed the phrase "Internet governance" itself, are quite new and subject to diverse interpretations by many communities of interest. As such, the definition is susceptible to being a vehicle for advancing parochial interests as opposed to a broad and encompassing definition that was the apparent object of the WGIG's undertaking.

Although the proposed definition may illuminate the aspirations of the WGIG's work, it does not take on substance or meaning until it is read in the context of existing entities and the global, regional, and national legal and regulatory systems that already provide necessary and significant principles, norms, rules, decision-making procedures and programs for the Internet infrastructure. These existing entities and systems are recognized in the WGIG report and were the focus of the third prong of WGIG's mandate. Hence, it is VeriSign's view that a process seeking to assess the state of Internet governance must be informed by the existing evolved mechanisms and institutions. The operating principles of a credible exercise must seek a comprehensive understanding of the existing entities and systems that currently deal with the wide variety of Internet administrative and public policy issues; this understanding should inform the working definition of "Internet governance" as opposed to the proposed definition informing or reordering these existing entities and systems.

B. <u>Public policy issues</u>

The WGIG report has identified four public policy areas:

- Issues relating to infrastructure and the management of critical Internet resources, including administration of the domain name system and Internet Protocol addresses (IP addresses), administration of the root server system, technical standards, peering and interconnection, telecommunications infrastructure, including innovative and convergent technologies, as well as multilingualization.

- Issues related to the use of the Internet, including spam, network security and cybercrime. While these issues are directly impacted by Internet governance, the nature of global cooperation required is not well defined.

- Issues that are relevant to the Internet but have an impact much wider than the Internet and for which existing organizations are responsible, such as intellectual property rights (IPRs) or international trade.

- Issues relating to the developmental aspects of Internet governance, in particular capacity-building in developing countries.

VeriSign submits that this aspect of the WGIG report can be distilled into two distinct categories: (1) name and address administration and related services operations associated with IETF RFC standards; and 2) generic public policy issues applicable to communication infrastructures. The first category—name-and-address administration—has evolved over the past decade through a private sector led, public-private partnership that has facilitated the rapid, global proliferation of the Internet infrastructure in a secure and stable manner. Indeed, considering the expansion of the use of Internet names and connected host computers over the last ten year period, it is a testament to the public-private model that the Internet has scaled on a global basis without any fundamental or systemic interruption. Moreover, this model has created an environment that encourages private sector innovation that is driving the development of next generation networks and services.

As an operator of critical DNS infrastructure, VeriSign understands the requirements for the "stability and security" of the DNS and, in particular, root server management. In view of the enormous economic and national security dependencies on the public Internet that have evolved over the past decade it is more than a casual suggestion that the design and operation of critical, high availability name server infrastructure continues to be best left to the incumbent technical experts rather than being redelegated to untested U.N. political bodies.

In addition to name and address administration, the WGIG report also identifies the following "highest priority" public policy issues: interconnection costs, Internet stability, security and cybercrime, spam, meaningful participation in global policy development, capacity building, intellectual property rights (IPR), freedom of expression, data protection and privacy rights, consumer rights and multilingualism.

With regard to these public policy issues, governments unquestionably have a definitive role to play in developing laws, regulations, norms, rules and decision-making processes by which they are addressed. In fact, governments already play an active role in Internet related public policy issues, as documented in the WGIG report. VeriSign welcomes encourages and recognizes the essential contributions of government participation in addressing these critical issues. Indeed, VeriSign participates in many government-sponsored collaborative efforts open to industry participants.

The focus of this debate should not be whether there is a role for government in Internet policy, but rather the manner in which governments collaborate in the future with the private sector and civil society in addressing Internet related public policy issues. The first step in that analysis is to recognize that the Internet has indeed challenged certain commercial and social constructs and is having a transformational impact on the manner in which countries, companies, and individuals communicate and interact. The second step is to recognize the unique benefit that the industry led public-private partnership has borne for DNS administration. The third step is to understand that the disruptive and enabling nature of the Internet provides an unparalleled opportunity to reshape the

relationship and collaboration between governments, the private sector, and civil society under an evolving concept of Internet governance.

The WGIG report has identified certain public policy issues that should be addressed by governments in a collaborative manner with the private sector and civil society. All participants in this process, including governments, however, must recognize the panoply of entities and systems that currently address, albeit not exhaustively for all issues, public policy matters identified by the WGIG report. Governments, the private sector, and civil society need to more fully understand the identity and role of the varied entities which address the broad range of public policy issues that are identified in the WGIG report.

While the WGIG report has identified a number of public policy issues, as cited above, VeriSign does not offer comments on all of the issues raised in the report. Rather, VeriSign offers observations on certain of these issues to identify critical considerations for the forward going dialogue among WSIS participants.

Internet stability, security and cybercrime

The WGIG report cites the lack of multilateral mechanisms to ensure the network stability and security of Internet infrastructure services and applications. The report also cites the lack of efficient tools and mechanisms to be used by countries to prevent and prosecute crimes committed in other jurisdictions, using technological means that might be located within or outside the territory where the crime had a negative effect.

With regard to the first point, national governments already play an important collaborative role in ensuring network stability and security. In fact, the infrastructure of the Internet which sustains the network's stability and security consists of a wide range of elements in addition to the DNS, which operate with less visibility, but no less efficiency and effectiveness than the DNS. These infrastructures—both physical and logical—include backbones, switching, global and regional peering points and subnetwork routing facilities, operated by dozens of private entities that cooperate with each other through standards activities, contractual arrangements and other institutional and informal cooperative arrangements. When one truly recognizes the multitude of infrastructures and entities that constitute "the Internet," it becomes clear that no one government exerts control over the Internet and that collaboration of a broad and, in some cases, highly specialized nature is already in place. Additionally, with the backdrop of 9/11 and other terrorist attacks around the world, the role for government participation in addressing security considerations across the broad range of Internet infrastructures is self-evident, but clearly not exclusive.

National governments must recognize that, with regard to the "stability and security" of the relatively narrow aspect of DNS administration, it is the industry led public-private model that has facilitated the operation and coordination of this key Internet infrastructure, and is responsible for the global roll out of the DNS in a stable and secure manner. While there are certainly areas where existing DNS administration can be

improved, there is no need to create new mechanisms to achieve that end. Where governments endeavor to improve and ensure Internet stability and security more broadly speaking, they should do so with the active and continuous participation of the private sector stewards of critical aspects of the Internet infrastructure.

With regard to the stated lack of efficient tools and mechanisms to be used by countries to prevent and prosecute Internet crimes, VeriSign encourages government engagement on this front and points to the Council of Europe Cybercrime Convention as an example where national governments have already collaborated constructively to provide a basis for law enforcement officials to address and prosecute criminal activity migrating to the Internet. VeriSign supports the ratification of the Cybercrime treaty by the United States Senate and by other countries that have not already done so, and the prompt development of national laws and law enforcement capabilities to effectuate commitments in the Convention.

VeriSign takes the most serious issue with positions which explicitly or implicitly attempt to link Internet crime, SPAM, or other consumer abuses with the fact of the present private-sector led administration of Internet infrastructure—be it the DNS or other infrastructure elements. Indeed, it is the same industry interests that have invented, developed, and deployed the lion's share of the Internet to date that have been among the leaders of initiatives to expand the capacity of nations to address and respond to abuses and crimes occurring on networks.[5] Indeed, VeriSign joins the growing body of commentators who believe abuses such as spam and identity theft are symptoms of failures in both deployments of adequate available technologies by users and network managers as well as failures of legal structures by host governments.
While increased government involvement and collaboration is required in this area, VeriSign notes that it is axiomatic that government regulatory mandates of technology generally (as in response to abuses) become less effective as they become more explicit and indeed hinder technological response to such abuses. Effective training of investigators and prosecutors, coupled with vigorous prosecution, are the best supplement to vigilant deployment of best-in-breed network security and data custody tools in combating the range of on-line fraud, crime, and consumer abuses such as SPAM.

Capacity-building

The development of local infrastructures, developers, and user populations is largely a combination of financial resources development, training of large populations of experts and the public-at-large. There are many excellent public and private mechanisms for accomplishing communications infrastructure development. Capacity building will be achieved through the purposeful establishment of market environments that provide

[5] See Letter to Sens. Richard G. Lugar, and Joseph R. Biden, Jr., United States Senate, on Convention on Cybercrime, dated June 29, 2005, signed by 15 companies and organizations; and, Information Technology Association of America, "Cyber Security Policy and Implementation: ITAA White Paper and Agenda," 2005.

incentives for private sector investment combined with the recognition by developed countries and their respective industries of the mutual long term benefits of expanding network infrastructures, knowledge transfer, and training in the developing world.

Data protection and privacy rights

The Report cites a "lack of existence or inconsistent application of privacy and data-protection rights," and "a lack of national legislation and enforceable global standards for privacy and data-protection rights over the Internet; as a result, users have few, if any, means to enforce their privacy and personal data-protection rights, even when recognized by legislation. An example of this is the apparent lack of personal data protection in some of the WHOIS databases."[6]

VeriSign notes that privacy and data protection have been the subject of significant legislative activity in a number of countries and geopolitical regions over the past few years. Privacy and data protection issues are colored by the history, culture, and economic models in a given country or region. In fact, there has been a fairly vigorous form of regulatory competition between different jurisdictions over privacy and data protections issues. The existence of this competition is not noted to support the notion that a single global privacy standard should be established or to suggest that there is a vacuum of engagement and participation. To the contrary, this on-going debate reflects serious engagement on this issue by governments, the private sector, and individuals alike.

This is an area where deeper involvement and collaboration among the various actors is needed. As with the security and cybercrime issues discussed above, the greatest opportunity for progress will come from aggressive deployment of best-in-breed data custody and network security tools by all institutions which are custodians of individual data; indeed, these improvements in data security practice may well begin with agencies of government themselves who are frequently the greatest aggregators of individual data and whose networks are frequently in greatest need of technology improvement. None of these important measures, however, require any alteration of the present industry-led administration of the DNS infrastructure.

What is urgently needed for both infrastructure protection and law enforcement support is the effective authentication of user and provider directories associated with the use of names and addresses. Not providing for the privacy mechanisms mentioned above exacerbates the ability to maintain authenticated, accurate directory information.

[6] Report of the Working Group on Internet Governance, pp. 7-8.

C. Develop a common understanding of the respective roles and responsibilities of all stakeholders in both developed and developing countries.

The third prong of the WGIG mandate is particularly constructive and is worthy of additional effort and collaboration among all interested parties. First, the work of the WGIG and, in particular, the International Chamber of Commerce (ICC), demonstrate that a wide array of organizations from across all sectors currently play an active role in addressing administration and policy issues concerning governance of the Internet. Indeed the work of cataloging every organization around the globe that currently plays a role in this area is likely incomplete.

Importantly, the WGIG work on this issue demonstrates that there is no vacuum within the context of existing structures to address Internet-related public policy issues. Governments, the private sector, and civil society can constructively collaborate to better understand the respective roles of the existing entities and structures. Effective collaboration will permit government and industry to identify ways in which the views of each can be recognized and harmonized. Existing entities can then cooperate in addressing many of the complex issues raised by the Internet and Internet usage.

Given the array of existing structures, the creation of a new entity would not result in improved efficiency or cover areas that are not already addressed. Developing countries that already have scarce resources would be adversely affected by the creation of yet another institution in which they would be prodded to participate. Even industries in developed countries find their resources stretched when trying to address the myriad of issues raised by the Internet and the emerging information society. The telecommunications industry is undergoing consolidation as it continues to recover from the "meltdown" of 2000, and the Internet services industry, albeit vibrant and important, is still relatively immature and lacking in the depth of resources typically associated with heavily regulated industries. Resources and effort would be much more wisely placed in collaborating to better understand how the respective players can build on existing structures to achieve important coordination and public policy goals.

III. CONCLUSIONS

A large global ecosystem of well-established and effective international multilateral, regional, national, and local forums already exists to treat "Internet governance." It is not apparent that an additional new forum is needed, or would usefully contribute to the objectives of the WSIS process. On the other hand, what does seem to be needed is more effective collaboration among existing organizations, effective participation in these organizations by interested parties, and ongoing dialogue among all the actors in question. The need for this collaboration and dialogue is underscored by the continuing integration of Internet infrastructure with wireless and existing public telecommunication infrastructures.

As the WSIS process moves forward and takes into account the WGIG report, the stability and security of the IP-enabled network infrastructure (especially the DNS) must continue to be its guiding principle. New models for top-level IETF RFC DNS administration are not warranted given the success of the industry- led, public- private partnership in the use and expansion of DNS infrastructure and services. Any model or discussion that encourages the creation of multiple, competing rules governing the root zone system would have a dangerous destabilizing effect on the stability and security of this critical infrastructure.